

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039794

(43)Date of publication of application : 12.02.1999

(51)Int.Cl.

G11B 20/10

(21)Application number : 09-192785

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 11.07.1997

(72)Inventor : KASHIWA HIROSHI

(54) DECIPHERING DEVICE OF CIPHERED DATA

(57)Abstract:

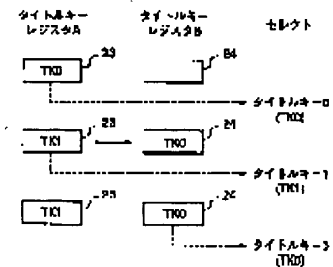
PROBLEM TO BE SOLVED: To quickly decipher ciphered data by deciphering ciphered data in data transmission between two points, i.e., 1 to 1 of an optical disk device recorded with ciphered data in a title key unit to a digital device equipped with a deciphering function of ciphered data, and also many to 1 of plural optical disk devices recorded with ciphered data in the title key unit to the digital device equipped with the deciphering function of ciphered data.

SOLUTION: An authenticating and data deciphering part is provided with plural title key registers A23 and B24, where plural title keys TK0 and TK1 are held respectively. When a data deciphering operation of a title 0 is performed again, data deciphering is carried out by selecting the title key register B24 holding the title key TK0 by a CPU without performing authenticating operation and a title key deciphering operation. Consequently, the time required for the authenticating operation to be performed at the time of deciphering the data of the same title key TK0 again is reduced, and hence the ciphered data can quickly be deciphered.

(11)

(02)

(03)



LEGAL STATUS

[Date of request for examination]

17.12.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-39794

(43) 公開日 平成11年(1999) 2月12日

(51) Int. Cl. 6

登録番号

特許

G 1 1 B 20/10

G 1 1 B 20/10

H

審査請求 未請求 請求項の数2 OL (全 10 頁)

(21) 出願番号 特願平9-192785

(22) 出願日 平成9年(1997) 7月17日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 柏 浩

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

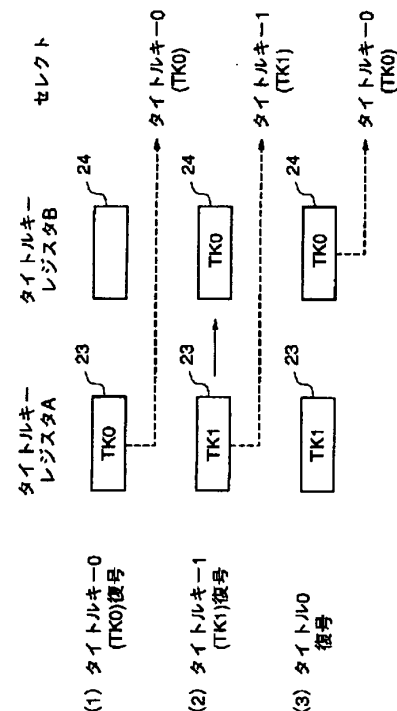
(74) 代理人 弁理士 早瀬 憲一

(54) 【発明の名称】 暗号データ復号装置

(57) 【要約】

【目的】 従来、複数のタイトルキーの暗号データが同一ディスク内に記録されている場合、タイトルキーが変わるごとに認証を行うため、1度復号したタイトルのデータでも認証が必要なため認証時間がかかり効率が悪かったため、この認証時間の短縮化を目的とする。

【解決手段】 認証・データ復号部2に複数のタイトルキーレジスタA 23、B 24を設け、それぞれに複数のタイトルキーTK0、TK1を保持しておく。再びタイトル0のデータ復号動作を行う場合、認証動作、タイトルキー復号動作を行なうことなくタイトルキーTK0を保持したタイトルキーレジスタB 24をCPU7が選択することでデータ復号を行なう。これにより、再び同じタイトルキーTK0のデータを復号する際に行われる認証動作にかかる時間が削減され、敏速な暗号データの復号を実現できる。



【特許請求の範囲】

【請求項1】 タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク装置とデジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって

上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのCPUデータを生成するCPUと、

上記光ディスク装置の暗号データを復号化する認証・データ復号部と、

上記認証・データ復号部によって復号化されたデジタルデータを記憶するメモリー手段とを備え、

上記認証・データ復号部は、

上記CPUまたは上記光ディスク装置からのCPUデータを復号処理する暗号・復号アルゴリズムと、

上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための1バイト以上の固定値の鍵である認証キー1を保持する認証キー1レジスタと、

上記認証ごとに变化する1バイト以上の鍵である認証キー2を保持する認証キー2レジスタと、

上記認証ごとに变化する1バイト以上の鍵である認証キー3を保持する認証キー3レジスタと、

上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、

上記暗号・復号アルゴリズムにより生成される異なる1バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、

上記暗号・復号アルゴリズムにおける鍵として上記認証キー1、上記認証キー2、上記認証キー3、上記タイトルキー復号キー、上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とする暗号データ復号装置。

【請求項2】 タイトル単位でタイトルキーの異なる暗号データを複数記録した複数の光ディスク装置とデジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、

上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのCPUデータを生成するCPUと、

上記光ディスク装置の暗号データを復号化する認証・データ復号部と、

上記認証・データ復号部によって復号化されたデジタルデータを記憶するメモリー手段とを備え、

上記認証・データ復号部は、

上記CPUまたは上記光ディスク装置からのCPUデータを復号処理する暗号・復号アルゴリズムと、

上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための1バイト以上の固定値の鍵である認証キー1を保持する認証キー1レジスタと、

上記認証ごとに变化する1バイト以上の鍵である認証キー2を保持する認証キー2レジスタと、

上記認証ごとに变化する1バイト以上の鍵である認証キー3を保持する認証キー3レジスタと、

上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、

上記複数の光ディスク装置から伝送される暗号データを復号するために各光ディスク装置のそれぞれに対応し、かつ、上記暗号・復号アルゴリズムにより生成される異なる1バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、

上記暗号・復号アルゴリズムにおける鍵として上記認証キー1、上記認証キー2、上記認証キー3、上記タイトルキー復号キー、上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とする暗号データ復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、2つのデジタル機器間の伝送または複数のデジタル機器の伝送においてタイトルと呼ばれる単位ごとに暗号化の鍵が異なり、かつタイトルが異なるごとに行う認証の時間短縮を実現する暗号データ復号装置に関するものである。

【0002】

【従来の技術】図1は、光ディスク装置とデジタルインターフェースを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図である。図1において、1は光ディスク装置、2は光ディスク装置側の認証部、3は光ディスク装置側のCPU、4は光ディスク、5は光ディスク装置側のインターフェース回路、6は暗号データ復号装置、7は暗号データ復号装置側のCPU、8は認証・データ復号部、9は暗号データ復号装置側のインターフェース回路、10はメモリー回路である。

【0003】暗号データ復号装置6は、タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク装置1とデジタルインターフェース手段5、9を用いたデータ伝送が行われ、かつ上記光ディスク装置1の暗号データを復号化するものである。この暗号データ復号装置6は、上記光ディスク装置1の暗号データを復号する際に通信主体の認証動作を行うためにCPUデータを生成するCPU7と、上記光ディスク装置1の暗号データを復号化する認証・データ復号部8と、上記光ディスク装置1とのデータ伝送を行うためのインターフェース回路9と、上記認証・データ復号部8によって復号

化されたデータを記憶するメモリー回路10とを備えたものである。

【0004】上記光ディスク装置1は、光ディスク4に記録された暗号データの認証を行う認証部2と、通信主体の認証動作を行うためにCPUデータを生成するCPU13と、タイトル単位でタイトルキーの異なる暗号データを複数記録した光ディスク4と、上記暗号データ復号装置6とのデータ伝送を行うためのインターフェイス回路5とを備えたものである。

【0005】図6は、従来の暗号データ復号装置6における認証・データ復号部8の構成を示すブロック図である。図6において、11はデータセクタ回路、12はタイトルキー復号のデータを保持するレジスタC、13は認証キー1レジスタ、14は認証キー2レジスタ、15は認証キー3レジスタ、16はタイトルキー復号キーレジスタ、17はタイトルキーレジスタ、18はキーセクタ回路、19は暗号・復号アルゴリズム(DES:特開昭51-108701号公報、特開昭51-108702号公報参照)、20は認証データを保持するレジスタA、21はコンパレータ回路、22は認証データを保持するレジスタBである。

【0006】以上のように構成された暗号データ復号装置6について、以下にその動作を説明する。なお、光ディスク装置1における認証部2の認証動作は、認証・データ復号部8と同じとする。上記光ディスク装置1のデータをインターフェイス回路5を用いて外部の暗号データ復号装置6で復号するためには、認証動作、タイトルキー復号動作、データ復号動作の順に行なう。

【0007】上記認証動作は、以下のステップ1～ステップ4の手順で行なう。まず、ステップ1として、暗号データ復号装置6のCPU7より発生した乱数Iを、認証・データ復号部8と、インターフェイス回路9により光ディスク装置1のCPU3を介して認証部2とに伝送する。認証・データ復号部8では、図6に示すように、データセクタ回路11においてCPUデータである上記乱数Iをデータとして選択し、かつ、キーセクタ回路18において認証キー1を鍵として選択し、暗号・復号アルゴリズム19による復号動作を行いその結果I(認証キー2)を認証キー2レジスタ14に保持する。また、光ディスク装置1の認証部2においても上記乱数Iをデータおよび認証キー1を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより認証キー2を生成する。

【0008】ステップ2として、光ディスク装置1のCPU3より発生した乱数IIを、認証部2と、インターフェイス回路5により暗号データ復号装置6のCPU7を介して認証・データ復号部8とに伝送する。認証・データ復号部8では、図6に示すように、データセクタ回路11においてCPUデータである上記乱数IIをデータとして選択し、かつ、キーセクタ回路18において認

証キー2レジスタ14を鍵として選択し、暗号・復号アルゴリズム19により復号動作を行いその結果II(認証キー3)を認証キー3レジスタ15に保持する。そして、光ディスク装置1の認証部2においても上記乱数IIをデータおよび認証キー2を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより認証キー2を生成する。

【0009】ステップ3として、暗号データ復号装置6のCPU7より発生した乱数IIIを、認証・データ復号部8と、インターフェイス回路9により光ディスク装置1のCPU3を介して認証部2とに伝送する。認証・データ復号部8では、図6に示すように、データセクタ回路11においてCPUデータである上記乱数IIIをデータとして選択し、かつ、キーセクタ回路18において認証キー3レジスタ15を鍵として選択し、暗号・復号アルゴリズム19により復号動作を行いその結果IIIをインターフェイス回路9により光ディスク装置1のCPU3を介して認証部2に伝送する。そして、光ディスク装置1の認証部2において上記乱数IIIをデータおよび認証キー3を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより生成された結果IVと、上記結果IIIの比較結果をCPU3に送り一致すれば光ディスク装置1における認証が成立する。

【0010】ステップ4として、光ディスク装置1のCPU3より発生した乱数IVを、認証部2と、インターフェイス回路5により暗号データ復号装置6のCPU7を介して認証・データ復号部8とに伝送する。そして、認証部2において上記乱数IVをデータとして認証キー3レジスタ15と同じデータを鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより生成された結果Vを、インターフェイス回路5によりCPU7を介して認証・データ復号部8に伝送し、その結果VをレジスタA20に保持する。認証・データ復号部8では、図6に示すように、データセクタ回路11においてCPUデータである上記乱数IVをデータとして選択し、かつ、キーセクタ回路18において認証キー3レジスタ14を鍵として選択し、暗号・復号アルゴリズム19により復号動作を行いその結果VIをレジスタB22に保持する。そして、コンパレータ回路21において上記レジスタA20に保持した結果Vと、上記レジスタB22に保持した結果VIとの比較結果をCPU7に送り一致すれば暗号データ復号装置6における認証が成立する。

【0011】このようにして、相互の認証が成立した所で、次のタイトルキー復号動作を行なうこととなる。タイトルキーは、タイトルキー復号キーを鍵として暗号・復号アルゴリズムを用いて暗号化して光ディスク4に記録している。したがって、例えば、タイトルキーAの復号は光ディスク4における再生したいタイトルAのタイトルキーAを、CPU3を介して認証部2へ送り、そのタイトルキーAをデータとして、認証キー2レジスタ1

4を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより暗号化し、その結果であるタイトルキーAをインターフェース回路5により暗号データ復号装置6へ伝送する。暗号データ復号装置6では、図6に示すように、伝送された上記タイトルキーAと認証キー2より暗号・復号アルゴリズム19を用いて復号動作を行いその結果をレジスタC12に保持する。次に、データセクタ回路11においてレジスタC12を選択し、かつ、キーセクタ18においてタイトルキー復号キー16を選択し、暗号・復号アルゴリズム19により復号動作を行いその結果であるタイトルキーAをタイトルキーレジスタ17に保持する。

【0012】上記タイトルキーの復号が終了した後に、以下のデータ復号動作を行なう。光ディスク4のデータは、タイトル単位でタイトルキーを鍵として暗号・復号アルゴリズムにより暗号化している。したがって、データの復号は光ディスク4より再生したいタイトルのデータをインターフェース回路5により暗号データ復号装置6の認証・データ復号部8に伝送する。認証・データ復号部8では、図6に示すように、データセクタ回路11においてインターフェース回路9からのデータを選択し、かつ、キーセクタ回路18においてタイトルキーレジスタ17を鍵として選択し、暗号・復号アルゴリズム19による復号動作を行い、ここで復号化されたデータはメモリー回路10に保持される。

【0013】以上のようにして、タイトルが変わるごとに上記認証動作、上記タイトルキー復号動作、上記データ復号動作を順次行なうことになる。

【0014】

【発明が解決しようとする課題】しかしながら、上記の従来の暗号データ復号装置の構成では、複数のタイトルキーで暗号化したデータが同一ディスク内に記録されている場合においてタイトルキーが変わるごとに認証を行うため、1度復号したタイトルキーに戻って暗号データを復号したい時も認証が必要のため認証時間がかかり効率が悪いということで問題点を有していた。

【0015】本発明は、上記従来の問題点を解決するためになされたものであり、要するに複数のタイトルキーを保持するレジスタを設けることにより、タイトルキー単位で暗号データが記録されている光ディスク装置と暗号データの復号機能を備えたデジタル装置の1対1、つまり2点間のデータ伝送における暗号データの復号化、およびタイトルキー単位で暗号データが記録されている複数の光ディスク装置と暗号データの復号機能を備えたデジタル装置の複数対1のデータ伝送における暗号データの復号化を敏速に行う暗号データ復号装置を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の請求項1に係る暗号データ復号装置は、タイトル単位でタイトルキーの

異なる暗号データを複数記録した光ディスク装置とデジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのCPUデータを生成するCPUと、上記光ディスク装置の暗号データを復号化する認証・データ復号部と、上記認証・データ復号部によって復号化されたデータを記憶するメモリー手段とを備え、上記認証・データ復号部は、上記CPUまたは上記光ディスク装置からのCPUデータを復号処理する暗号・復号アルゴリズムと、上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する、認証を行うための1バイト以上の固定値の鍵である認証キー1を保持する認証キー1レジスタと、上記認証ごとに变化する1バイト以上の鍵である認証キー2を保持する認証キー2レジスタと、上記認証ごとに变化する1バイト以上の鍵である認証キー3を保持する認証キー3レジスタと、上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、上記暗号・復号アルゴリズムにより生成される異なる1バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、上記暗号・復号アルゴリズムにおける鍵として上記認証キー1、上記認証キー2、上記認証キー3、上記タイトルキー復号キー、上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とするものである。

【0017】また、本発明の請求項2に係る暗号データ復号装置は、タイトル単位でタイトルキーの異なる暗号データを複数記録した複数の光ディスク装置とデジタルインターフェース手段を用いたデータ伝送が行われ、かつ上記光ディスク装置の暗号データを復号化する暗号データ復号装置であって、上記光ディスク装置の暗号データを復号する際に通信主体の認証動作を行うためのCPUデータを生成するCPUと、上記光ディスク装置の暗号データを復号化する認証・データ復号部と、上記認証・データ復号部によって復号化されたデジタルデータを記憶するメモリー手段とを備え、上記認証・データ復号部は、上記CPUまたは上記光ディスク装置からのCPUデータを復号処理する暗号・復号アルゴリズムと、上記暗号データのタイトルが変わるごとに通信主体の正当性を証明する認証を行うための1バイト以上の固定値の鍵である認証キー1を保持する認証キー1レジスタと、上記認証ごとに变化する1バイト以上の鍵である認証キー2を保持する認証キー2レジスタと、上記認証ごとに变化する1バイト以上の鍵である認証キー3を保持する認証キー3レジスタと、上記タイトルキーを復号するための鍵であるタイトルキー復号キーを保持するタイトルキー復号キーレジスタと、上記複数の光ディスク装置から伝送される暗号データを復号するために各光デ

ディスク装置のそれぞれに対応し、かつ、上記暗号・復号アルゴリズムにより生成される異なる1バイト以上のタイトルキーを保持する複数のタイトルキーレジスタと、上記暗号・復号アルゴリズムにおける鍵として上記認証キー1、上記認証キー2、上記認証キー3、上記タイトルキー復号キー、上記復号化したタイトルキーのいずれかを選択するキーセレクト手段とを有することを特徴とするものである。

【0018】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら説明する。

実施の形態1. 図1は、本発明の実施の形態1による、光ディスク装置とデジタルインターフェイスを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図であり、光ディスク装置1や暗号データ復号装置6のブロック構成は、従来のものと同様である。図2は、本実施の形態1による暗号データ復号装置6における認証・データ復号部8の構成を示すブロック図である。

【0019】実施の形態1は、光ディスク装置と暗号データ復号装置との1対1、つまり2点間のデジタルインターフェイスを用いたデータ伝送において、タイトル単位で暗号化したデータの円滑な復号化を行える暗号データ復号装置である。すなわち、実施の形態1の暗号データ復号装置6が、図6のブロック図に示した従来のものと異なるところは、従来のものではタイトルキーレジスタ17が1つしかなかったのに対し、実施の形態1のものでは図2に示すように、タイトルキーレジスタA23とタイトルキーレジスタB24と2つ有することである。

【0020】図3は、図2に示す如く、タイトルキーレジスタA23とタイトルキーレジスタB24とを2つ備えた場合の上記認証・データ復号部8のデータ復号図である。図3において、23はタイトルキーレジスタA、24はタイトルキーレジスタBである。また、TK0はタイトル0におけるタイトルキー、TK1はタイトル1におけるタイトルキーである。

【0021】以上のように構成された暗号データ復号装置について、以下にその動作を説明する。

【0022】まず、光ディスク装置1のデータをインターフェース回路5を用いて外部の暗号データ復号装置6で復号するには認証動作、タイトルキー復号動作、データ復号動作の順に行なう。

【0023】上記認証動作は、以下のステップ1～ステップ4の手順で行なう。タイトル0を再生するためには、まず、ステップ1として、暗号データ復号装置6のCPU7より発生した乱数Iを認証・データ復号部8とインターフェース回路9により光ディスク装置1のCPU3を介して認証部2とに伝送する。認証・データ復号部8では、図2に示すように、データセクタ回路11

においてCPUデータである上記乱数Iをデータとして選択し、かつ、キーセクタ回路18において認証キー1を鍵として選択し、暗号・復号アルゴリズム19による復号動作を行いその結果Iを認証キー2レジスタ14に保持する。また、光ディスク装置1の認証部2においても上記乱数Iをデータおよび認証キー1を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより認証キー2を生成する。

【0024】ステップ2として、光ディスク装置1のCPU3より発生した乱数IIを認証部2と、インターフェース回路5により暗号データ復号装置6のCPU7を介して認証・データ復号部8とに伝送する。認証・データ復号部8では、図2に示すように、データセクタ回路11においてCPUデータである上記乱数IIをデータとして選択し、かつ、キーセクタ回路18において認証キー2レジスタ14を鍵として選択し、暗号・復号アルゴリズム19により復号動作を行いその結果IIを認証キー3レジスタ15に保持する。また、光ディスク装置1の認証部2においても上記乱数IIをデータおよび認証キー2を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより認証キー3を生成する。

【0025】ステップ3として、暗号データ復号装置6のCPU7より発生した乱数IIIを認証・データ復号部8と、インターフェース回路9により光ディスク装置1のCPU3を介して認証部2とに伝送する。認証・データ復号部8では、図2に示すように、データセクタ回路11においてCPUデータである上記乱数IIIをデータとして選択し、かつ、キーセクタ回路18において認証キー3レジスタ15を鍵として選択し、暗号・復号アルゴリズム19により復号動作を行いその結果IIIを、インターフェース回路9により光ディスク装置1のCPU3を介して認証部2に伝送する。また、光ディスク装置1の認証部2において上記乱数IIIをデータおよび認証キー3を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより生成された結果IVと上記結果3の比較結果をCPU3に送り一致すれば光ディスク装置1における認証が成立する。

【0026】ステップ4として、光ディスク装置1のCPU3より発生した乱数IVを認証部2と、インターフェース回路5により暗号データ復号装置6のCPU7を介して認証・データ復号部8に伝送する。また、認証部2において上記乱数IVをデータとして認証キー3レジスタ15と同じデータを鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより生成された結果Vを、インターフェース回路5によりCPU7を介して認証・データ復号部8に伝送し、レジスタA20に保持する。認証・データ復号部8では、図2に示すように、データセクタ回路11においてCPUデータである上記乱数IVをデータとして選択し、かつ、キーセクタ回路18において認証キー3レジスタ14を鍵として選択し、暗

号・復号アルゴリズム19により復号動作を行いその結果VIをレジスタB22に保持し、コンパレータ回路21においてレジスタA20とレジスタB22の比較結果をCPU7に送り一致すれば暗号データ復号装置6における認証が成立する。このようにして、相互の認証が成立した所で、タイトル0のタイトルキー復号動作を行なうこととなる。

【0027】タイトルキーTK0は、タイトルキー復号キーを鍵として暗号・復号アルゴリズムを用いて暗号化して光ディスク4に記録している。したがって、タイトルキーTK0の復号は光ディスク4における再生したいタイトル0のタイトルキーTK0をCPU3を介して認証部2へ送り、タイトルキーTK0をデータとして、認証キー2レジスタ14を鍵として用いて暗号・復号アルゴリズム19と同じアルゴリズムにより暗号化した結果であるタイトルキーTK0をインターフェース回路5により暗号データ復号装置6へ伝送する。暗号データ復号装置6では伝送された上記タイトルキーTK0と認証キー2より暗号・復号アルゴリズム19を用いて復号動作を行いその結果をレジスタC12に保持する。次に、データセクタ回路11においてレジスタC12を選択し、かつ、キーセクタ回路18においてタイトルキー復号キー16を選択し、暗号・復号アルゴリズム19により上記タイトル0のデータの複合に必要なタイトルキーTK0のタイトルキー復号動作を行いその結果を、図3(1)に示すように、タイトルキーレジスタA23に保持する。上記タイトルキーTK0の復号が終了後に、上記タイトル0のデータ復号動作を行なう。

【0028】光ディスク4のデータは、タイトル単位でタイトルキーを鍵として暗号・復号アルゴリズムにより暗号化している。したがって、タイトル0のデータの復号は光ディスク4より再生したいタイトル0のデータをインターフェース回路5により暗号データ復号装置6の認証・データ復号部8に伝送する。認証・データ復号部8では、図2に示すように、データセクタ回路11においてインターフェース回路9からのデータを選択し、かつ、キーセクタ回路18においてタイトルキーレジスタA23を鍵として選択し、暗号・復号アルゴリズム19によりタイトル0のデータの復号動作を行い、そして復号化されたタイトル0のデータはメモリー回路10に保持される。

【0029】次に、タイトル1を再生するために、上記認証動作を行い、上記タイトル1のデータの復号に必要なタイトルキーTK1を上記タイトルキー復号動作によりタイトルキーレジスタA23に保持し、上記タイトルキーレジスタA23を鍵として上記データ復号動作により上記タイトル1のデータを復号する。この時、図3(2)に示すように、上記タイトル0のタイトルキーTK0をタイトルキーレジスタA23からタイトルキーレジスタB24に移し保持する。このようにして、順次新し

いタイトルキーTK2, TK3, ...を復号すると同時にタイトルキーレジスタA23に保持すると同時にタイトルキーレジスタA23にあったタイトルキーTK1, TK2, ...をタイトルキーレジスタB24に移し保持する。

【0030】ここで、新たに上記タイトル0のデータ復号動作を行いたい場合は、上記認証動作および上記タイトルキー復号動作を行なうことなく、図3(3)に示すように、上記CPU7がタイトルキーレジスタB24を選択することで、タイトル0のデータの復号を行なう。

【0031】このように、本実施の形態1による暗号データ復号装置6によれば、タイトルキーレジスタA23、タイトルキーレジスタB24を選択することで上記認証動作および上記タイトルキー復号動作を行なうことなく、光ディスク装置1のデータの復号を行なうので、タイトルキー単位で暗号データが記録されている光ディスク装置と暗号データの復号機能を備えたデジタル装置の1対1、つまり2点間のデータ伝送における暗号データの復号化を敏速に行うものが実現できるという効果がある。

【0032】実施の形態2. 図4は、本実施の形態2による暗号データ復号装置6における認証・データ復号部8の構成を示すブロック図である。図5は、図4に示す如く、タイトルキーレジスタA23とタイトルキーレジスタB24とタイトルキーレジスタC25とを3つ備えた場合の上記認証・データ復号部8のデータ復号図である。図5において、26は光ディスク装置A、27は光ディスク装置B、28は光ディスク装置C、23はタイトルキーレジスタA、24はタイトルキーレジスタB、25はタイトルキーレジスタCである。また、TKAはタイトルAにおけるタイトルキー、TKBはタイトルBにおけるタイトルキー、TKCはタイトルCにおけるタイトルキーである。

【0033】実施の形態2は、3台の光ディスク装置と暗号データ復号装置との3対1でのデジタルインターフェイスを用いたデータ伝送において、タイトル単位で暗号化したデータの円滑な復号化を行える暗号データ復号装置である。すなわち、実施の形態2による暗号データ復号装置は、図4、図5に示すように、3台の光ディスク装置A、B、Cと暗号データ復号装置6の3対1でのタイトルキーレジスタを3つ(タイトルキーレジスタA23, B24, C25)備えた場合における上記認証・データ復号部8を有するものである。

【0034】次に、実施の形態2による暗号データ復号装置6の動作を説明する。まず、光ディスク装置A26、光ディスク装置B27、光ディスク装置C28の順にデータの復号を行う。光ディスク装置A26のタイトルAを再生するために、上記実施の形態1で説明したときと同様に、上記認証動作を行い上記タイトルAのデータの復号に必要なタイトルキーTKAを上記タイトルキ

一復号動作によりタイトルキーレジスタA23に保持し、上記タイトルキーレジスタA23を鍵として上記データ復号動作により上記タイトルAのデータを復号する。

【0035】同様に、光ディスク装置B27のタイトルBを再生するために、上記認証動作を行い、上記タイトルBのデータの復号に必要なタイトルキーTKBを上記タイトルキー復号動作によりタイトルキーレジスタB24に保持し、上記タイトルキーレジスタA24を鍵として上記データ復号動作により上記タイトルBのデータを復号する。

【0036】また、光ディスク装置C28のタイトルCを再生するために、上記認証動作を行い、上記タイトルCのデータの復号に必要なタイトルキーを上記タイトルキー復号動作によりタイトルキーレジスタC25に保持し、上記タイトルキーレジスタC25を鍵として上記データ復号動作により上記タイトルCのデータを復号する。

【0037】なお、上記実施の形態1では、図3に示すように、予めタイトルキーレジスタA23にタイトルキーTK0が保持されている場合、次にタイトル1のデータを復号するとき、このタイトルキーTK0をタイトルキーレジスタB24に移していたが、実施の形態2では、3台の光ディスク装置にそれぞれ対応してタイトルキーレジスタが1つずつ設けられているものであるため、このようなタイトルキーの移動は行われない。

【0038】次に、例えば、光ディスク装置C28の上記タイトルCのデータ復号後に、光ディスク装置A26の上記タイトルAを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、CPU7がタイトルキーレジスタA23を選択することで上記タイトルAのデータを復号し、また、光ディスク装置B27の上記タイトルBを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、CPU7がタイトルキーレジスタB24を選択することで上記タイトルBのデータを復号し、さらに、光ディスク装置C28の上記タイトルCを復号する場合には上記認証動作および上記タイトルキー復号動作を行なうことなく、CPU7がタイトルキーレジスタC25を選択することで上記タイトルCのデータを復号する。

【0039】このように、本実施の形態2による暗号データ復号装置によれば、3台の光ディスク装置A26、B27、C28のそれぞれの最後にアクセスしたタイトルキーTKA、TKB、TKCをタイトルキーレジスタA23、タイトルキーレジスタB24、タイトルキーレジスタC25に保持し、タイトルキーレジスタA23、タイトルキーレジスタB24、タイトルキーレジスタC25のいずれかを選択することで上記認証動作および上記タイトルキー復号動作を行なうことなく、光ディスク装置A26、光ディスク装置B27、光ディスク装置C

28のデータの復号を行なうので、タイトルキー単位で暗号データが記録されている複数の光ディスク装置と暗号データの復号機能を備えたデジタル装置の複数対1のデータ伝送における暗号データの復号化を敏速に行うものを実現できるという効果がある。

【0040】なお、本発明に係る暗号データ復号装置

は、上記実施の形態2のものでは、光ディスク装置A26、B27、C28のそれぞれに対応したタイトルキーレジスタが1つずつ設けられているものであるが、この実施の形態2のものにおいて、例えば、上記実施の形態1の如く、光ディスク装置A26、B27、C28のそれぞれに対応したタイトルキーレジスタが複数個ずつ設けられているものであってもよい。また、実施の形態2では、3台の光ディスク装置との間でデジタルインターフェイスを用いたデータ伝送を行うものであるが、本発明に係る暗号データ復号装置にあっては、任意の複数台の光ディスク装置との間でデジタルインターフェイスを用いたデータ伝送を行うものであってもよい。

【0041】

【発明の効果】以上のように、本発明の請求項1に係る暗号データ復号装置によれば、暗号・復号アルゴリズムにより生成される異なる1バイト以上のタイトルキーを2つ以上保持するレジスタを備えることにより、タイトルキーと呼ばれる鍵を用いて暗号化したデータを複数記録した光ディスク装置からデジタル伝送される暗号データの復号機能を備えたデジタル装置（暗号データ復号装置）への1対1、つまり2点間のデジタルインターフェイスを用いたデータ伝送において、1度復号したタイトルキーに戻って暗号データを復号したい時に認証動作することなく復号でき、これにより、暗号データの復号化を敏速に行えるものが実現できるという効果がある。

【0042】また、本発明の請求項2に係る暗号データ復号装置によれば、複数の光ディスク装置と暗号データの復号機能を備えたデジタル装置（暗号データ復号装置）の複数対1のデータ伝送において、複数の光ディスク装置のそれぞれがアクセスしたタイトルキーを保持することで再び同じタイトルキーの光ディスク装置のデータを復号する場合に認証動作することなく復号でき、これにより、暗号データの復号化を敏速に行えるものが実現できるという効果がある。

【図面の簡単な説明】

【図1】 実施の形態1、および従来における、光ディスク装置とデジタルインターフェイスを用いてデータ伝送が行われる暗号データ復号装置の構成を示すブロック図である。

【図2】 実施の形態1による暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

【図3】 実施の形態1による暗号データ復号装置の認

証・データ復号部におけるデータ復号図である。

【図4】 実施の形態2による暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

【図5】 実施の形態2による暗号データ復号装置の認証・データ復号部におけるデータ復号図である。

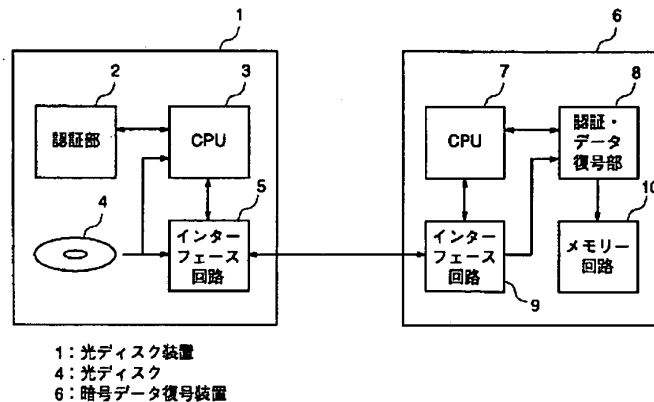
【図6】 従来の暗号データ復号装置の認証・データ復号部における構成を示すブロック図である。

【符号の説明】

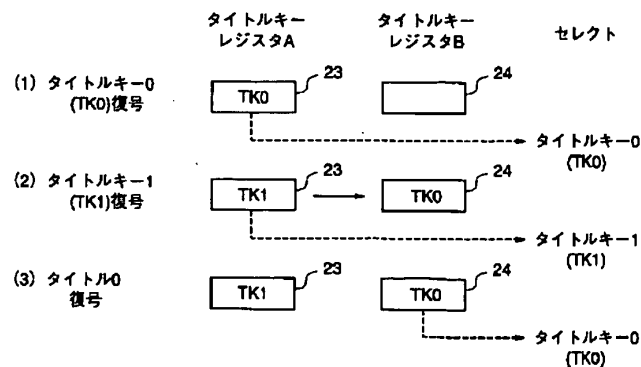
- 1 光ディスク装置
- 2 認証部
- 3 CPU
- 4 光ディスク
- 5 光ディスク装置におけるインターフェース回路
- 6 暗号データ復号装置
- 7 CPU
- 8 認証・データ復号部
- 9 暗号データ復号装置におけるインターフェース回路
- 10 メモリー回路

- 11 データセクタ回路
- 12 レジスタC
- 13 認証キー1レジスタ
- 14 認証キー2レジスタ
- 15 認証キー3レジスタ
- 16 タイトルキー復号キーレジスタ
- 17 タイトルキーレジスタ
- 18 キーセクタ回路
- 19 暗号・復号アルゴリズム
- 20 レジスタA
- 21 コンパレータ回路
- 22 レジスタB
- 23 タイトルキーレジスタA
- 24 タイトルキーレジスタB
- 25 タイトルキーレジスタC
- 26 光ディスク装置A
- 27 光ディスク装置B
- 28 光ディスク装置C

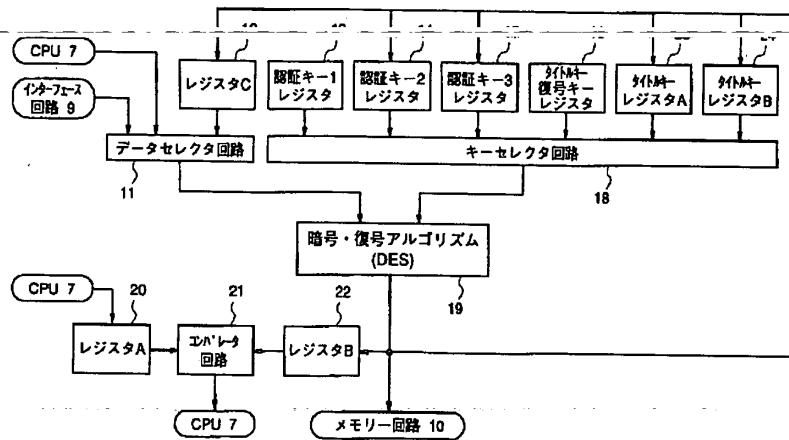
【図1】



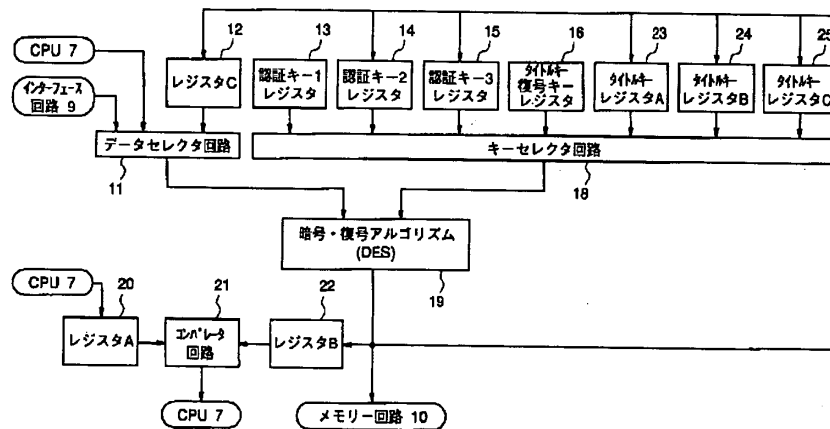
【図3】



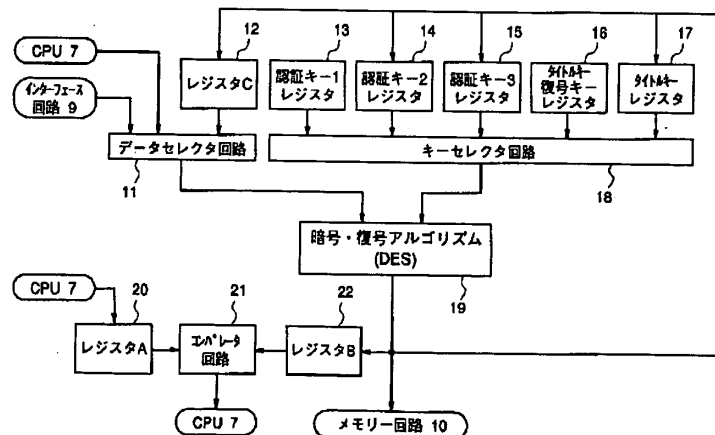
【図2】



【図4】



【図6】



【図5】

